

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

JUN 12 1998

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

ORIGINAL

In the Matter of)
)
Communications Assistance) CC Docket No. 97-213
For Law Enforcement Act)

REPLY COMMENTS OF THE
CENTER FOR DEMOCRACY AND TECHNOLOGY

James X. Dempsey, Senior Staff Counsel
Daniel J. Weitzner, Deputy Director
Center for Democracy and Technology
1634 Eye Street, N.W., Suite 1100
Washington, D.C. 20006
(202) 637-9800
www.cdt.org

Martin L. Stern
Michael J. O'Neil
Lisa A. Leventhal
Preston Gates Ellis & Rouvelas
Meeds LLP
1735 New York Avenue, N.W., Suite 500
Washington, D.C. 20006
(202) 628-1700

Attorneys for Center for Democracy and Technology

Dated: June 12, 1998

No. of Copies rec'd
List ABCDE

013

SUMMARY

The Federal Bureau of Investigation and the Department of Justice claim that the underlying wiretap laws are sufficient to protect the privacy interests implicated by CALEA's implementation. The enhanced surveillance capabilities the government seeks, however, would in no way be mitigated by the existing privacy protections in Title III and the Electronic Communications Privacy Act, but actually would circumvent some of their basic assumptions and protections.

There are two major problems with the government's theory that the request for excessive surveillance capabilities is ameliorated by Title III's "minimization" requirement. First, minimization requirements do not apply to pen registers or trap and trace devices, by which law enforcement would capture much of the information under dispute in this proceeding. Second, in CALEA, Congress imposed a separate "minimization" requirement *on carriers* so that, for the first time, carriers are required to affirmatively design their systems to protect the privacy and security of communications not authorized to be intercepted.

Most of the controversy over CALEA does not implicate the interception of call content under the standards set forth in Title III, but rather concerns interceptions conducted under the separate standard which governs the capture of the numbers dialed on outgoing and incoming calls. In contrast to the Fourth Amendment probable cause standard of Title III, the standard for such pen registers and trap and trace devices is strikingly low. It is critical to the Commission's understanding of the assistance capability standards issue to appreciate that every item contained in the FBI's punch list, with the exception of one, would be obtainable under this negligible standard.

Even more shocking, however, is the fact that the packet surveillance provision of the interim industry standard, which CDT has challenged, would also allow law enforcement to acquire the full content of a person's communications under this minimal standard. Accordingly, individual law enforcement agents would have absolute discretion, with no judicial supervision, to determine what information they are legally allowed to keep and what information they are legally required to ignore.

This is not what Congress had in mind in CALEA nor what the law requires. This acquisition of information not otherwise authorized by legal process is not just a matter of technical convenience. Rather, allowing such broad access to information would evade the fundamental Constitutional protections required in the case of Fourth Amendment searches, which are embodied in Title III.

There is, of course, another consideration that must be accounted for in implementing the Act: cost. At the end of the day, except for the narrowly circumscribed capabilities set forth in the Act, market forces and carrier decisions must drive the design of capabilities available to law enforcement, not government fiat.

The Commission must make a substantive judgment, based on a careful reading of the statutory language and legislative history, as to the type of CALEA standard that meets the statutory criteria. Furthermore, the Commission must adopt a standard that balances privacy interests against what the government asserts (and will always assert) is information essential for law enforcement purposes. The underlying issue is whether the CALEA standard eventually adopted by the Commission should provide the broad technical access sought by the government, or whether, as Congress directed, carriers should be required only to preserve a basic surveillance access fitting within the four corners of the legislative language.

TABLE OF CONTENTS

SUMMARY	i
INTRODUCTION	1
DISCUSSION	6
I. THE PRIVACY PROTECTIONS OF TITLE III, ECPA AND CALEA.....	6
A. The Distinction Under Title III Between Call Content and Dialing Information ...	7
B. The Government’s Approach to CALEA Would Impermissibly Expand Information Available Under a Pen Register Authorization.....	11
II. THE GOVERNMENT FAILS TO RECOGNIZE CALEA’S BUILT-IN LIMITATIONS.....	13
III. CALEA MUST BE NARROWLY INTERPRETED IN ACCORDANCE WITH ITS PLAIN MEANING	16
A. Words Cannot be Added to the Act	17
B. A Particular Word in a Particular Clause Cannot have Multiple Meanings	17
IV. THE GOVERNMENT’S APPROACH TO CONFERENCE CALLS VIOLATES FUNDAMENTAL TITLE III PRINCIPLES.....	18
CONCLUSION	22

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of)	
)	
Communications Assistance)	CC Docket No. 97-213
For Law Enforcement Act)	

**REPLY COMMENTS OF THE
CENTER FOR DEMOCRACY AND TECHNOLOGY**

Pursuant to the April 20, 1998 Public Notice, DA 98-762, ("Public Notice") in the captioned docket, the Center for Democracy and Technology ("CDT"), by its undersigned attorneys, hereby submits its reply comments on the scope of the assistance capability requirements necessary to satisfy the obligations imposed by the Communications Assistance for Law Enforcement Act (the "Act" or "CALEA")¹ and the responsibility of the Commission to ensure that the Act is implemented in a way that protects the privacy of the American people.

INTRODUCTION

In response to CDT's Petition (filed March 25, 1998), the Federal Bureau of Investigation and the Department of Justice ("FBI," "DOJ," or collectively, the "government") claim that the underlying wiretap laws are sufficient to protect the privacy interests that are obviously implicated by the implementation of CALEA. In this Reply, CDT will respond to the

¹ Pub. L. No. 103-414, 108 Stat. 4279 (1994), codified at 47 U.S.C. §§ 1001-1010 and in various sections of Title 18 and Title 47.

government's erroneous assertion by first describing several pertinent aspects of the wiretap laws, an area not normally reviewed by the Commission. CDT will also explain how the enhanced surveillance capabilities the government seeks would in no way be mitigated by the existing privacy protections in Title III and the Electronic Communications Privacy Act ("ECPA"), but actually would circumvent some of their basic assumptions and protections.

The government's justification for excessive surveillance capabilities hinges greatly on Title III's "minimization" requirement. Title III requires that law enforcement conduct wiretaps "in such a way as to *minimize* the interception of communications not otherwise subject to interception."² However, there are two major problems with the government's theory. First, the "minimization" requirement, as well as judicial supervision of compliance with Title III, do not apply to pen registers or trap and trace devices, by which law enforcement would capture much of the information under dispute in this proceeding. Second, in CALEA, Congress imposed a separate "minimization" requirement *on carriers* so that, for the first time, carriers are required to affirmatively design their systems to protect the "privacy and security of communications . . . not authorized to be intercepted."³

As others have noted, most of the controversy over CALEA does not implicate the interception of call content under the standards set forth in Title III,⁴ but rather concerns interceptions conducted under the separate standard governing pen registers and trap and trace devices, which capture the numbers dialed on outgoing and incoming calls, respectively.⁵ In

² 18 U.S.C. § 2518(5)(emphasis added).

³ 47 U.S.C. § 1002(a)(4).

⁴ Title III, 18 U.S.C. § 2510 *et seq.*

⁵ 18 U.S.C. § 3121 *et seq.*

contrast to the Fourth Amendment probable cause standard of Title III, the standard for pen registers and trap and trace devices is strikingly low. The standard does not involve probable cause at all but merely requires that the intercepted information be “*relevant* to an ongoing criminal investigation.”⁶ Furthermore, courts have absolutely no discretion to deny an application for a pen register or trap and trace order as long as it is signed by a prosecutor or a state or local police officer. Moreover, courts have no authority to question the factual basis for the application. And, finally, once the order is approved, there is no ongoing judicial supervision and no return of service to the court and, thus, there is no ability to ensure that law enforcement acted properly in carrying out the order.

It is critical to the Commission’s understanding of the assistance capability standards issue to appreciate that every item contained in the FBI’s punch list, with the exception of one, would be obtainable under this negligible pen register standard. Even more shocking, however, is the fact that the packet surveillance provision of the interim industry standard, which CDT has challenged, would also allow law enforcement to acquire the full content of a person’s communications under this minimal standard. Accordingly, individual local, state and federal law enforcement agents would have absolute discretion, with no judicial supervision, to determine what information they are legally allowed to keep and what information they are legally required to ignore.

The government argues that this ad-hoc, unsupervised determination is appropriate under CALEA and the Commission should allow carriers to give law enforcement a virtual fire hose of data, leaving it to them to figure out how to protect “the privacy and security of communications

⁶ 18 U.S.C. § 3123(a)(emphasis added).

and call-identifying information not authorized to be intercepted."⁷ However, this is not what Congress had in mind nor what the law requires. Congress deferred the implementation of CALEA to the standard setting process initially, but, upon petition from any person, it is the Commission that must determine how to properly balance privacy with the insistence of the government that additional data, although not authorized to be intercepted, should be provided anyway because some other statute or process will prevent governmental abuse. This acquisition of information not otherwise authorized by legal process is not just a matter of technical convenience, which a proper judicial order can subsequently correct. Rather, allowing such broad access to information would evade the fundamental Constitutional protections required in the case of Fourth Amendment searches, which are embodied in Title III.

In sum, the government argues that a pen register in analog systems provides content today. This argument ignores, however, the privacy protection obligation imposed under Section 103(a)(4) of CALEA, which mandates carriers to avoid such practices in CALEA-compliant systems. Moreover, the government misses the key fact that the capabilities the government proposes be built into the nation's telecommunications networks under CALEA would provide a flood of constitutionally-protected information that goes well beyond anything that has historically been available to law enforcement under a pen register or trap and trace authority.

There is, of course, another consideration that must be accounted for in implementing the Act: cost. Capabilities that go beyond CALEA's requirements drive up costs for carriers. Ultimately, however, it is the consumer that will pay for the additional intrusion of such technology, which is another reason why Congress wanted CALEA implementation decisions to

⁷ 47 U.S.C. § 1002(a)(4).

be regulated by a balancing test. Since everything CALEA mandates results in costs to carriers and consumers, Congress established minimum requirements that were also to act as a ceiling on what could be required of carriers. Therefore, the Commission must ensure that any standard it establishes "meet[s] the assistance capability requirements of section 103 by cost-effective methods" as well as "protect[s] the privacy and security of communications not authorized to be intercepted."⁸ At the end of the day, except for the narrowly circumscribed capabilities set forth in the Act, market forces and carrier decisions must drive the design of capabilities available to law enforcement, not government fiat.

The Commission must make a substantive judgment, based on a careful reading of the statutory language and legislative history, as to the type of CALEA standard that meets the statutory criteria. Furthermore, the Commission must adopt a standard that balances privacy interests against what the government asserts (and will always assert) is information essential for law enforcement purposes. The underlying issue is whether the CALEA standard eventually adopted by the Commission should provide the broad technical access sought by the government, or whether, as Congress directed, carriers should be required only to preserve a basic surveillance access fitting within the four corners of the legislative language.

⁸ 47 U.S.C. § 1006(b)(1) and (2).

DISCUSSION

I. THE PRIVACY PROTECTIONS OF TITLE III, ECPA AND CALEA

In response to CDT's objections to provisions of the industry standard and the punch list, the FBI and DOJ seem to admit that these provisions do pose privacy concerns, but they argue that the wiretap laws themselves adequately address those privacy issues. It is clear, however, that Congress concluded that the protections of Title III and ECPA were *not* adequate to deal with the privacy concerns raised by the design mandates of CALEA. Otherwise Congress would have given the FBI, DOJ, or this Commission authority to mandate any and all surveillance features desired by law enforcement, without limitation.⁹ If this was its intention, Congress certainly would not have imposed in Section 103(a)(4) of the Act a *new* and *separate* obligation on carriers to protect the privacy of communications not authorized to be intercepted.

In its May 20 Comments, CDT outlined the history and context of the wiretap laws in order to show that CALEA was intended to preserve a historical balance between privacy and law enforcement interests. From the government's Comments, it is clear that it would also be useful to outline the relevant assumptions and standards of Title III's wiretap laws to explain the relationship between those standards and the minimum requirements of CALEA.

⁹ The Commission should, of course, look to the privacy protections in the wiretap laws, for CALEA obviously cannot be interpreted to mandate surveillance features the use of which could not be authorized under Title III or ECPA. This means, for example, that CALEA cannot mandate the conference calling capability sought by the FBI, since, as we will explain below, Title III and ECPA do not authorize the interception of unknown persons not suspected of being involved in criminal conduct and using facilities not specified in the interception order merely because they previously were on a conference call with the target of the surveillance.

A. The Distinction Under Title III Between Call Content and Dialing Information

Title III and Supreme Court precedent in wiretap cases have always drawn a distinction between the content of communications and the dialed number information collected under pen registers and trap and trace devices.

In 1967, the Supreme Court held that interception of the content of telephone conversations was a search and seizure under the Fourth Amendment.¹⁰ Congress responded one year later by adopting Title III, which, consistent with the Fourth Amendment, requires a prior judicial order issued on a finding of probable cause for the government to intercept the content of wire or oral communications.¹¹

Due to the unique intrusiveness of wiretapping, Congress imposed in Title III additional restrictions on eavesdropping, limiting it to certain serious offenses, 18 U.S.C. § 2516; requiring prior exhaustion of other less intrusive investigative techniques before a warrant is issued, 18 U.S.C. § 2518(1)(c) and (3)(c); requiring high level Justice Department approval for all applications, 18 U.S.C. § 2516; requiring law enforcement to “minimize” the capture of innocent conversations, 18 U.S.C. § 2518(5); and, finally, requiring close judicial supervision of the progress of interceptions, 18 U.S.C. § 2518(6) and (8).

Title III, however, does not govern the use of pen registers or trap and trace devices, which capture numbers dialed on outgoing or incoming calls, respectively.¹² In 1979, the Supreme Court, in *Smith v. Maryland*, 442 U.S. 735 (1979), held that the installation and use of a

¹⁰ *Katz v. United States*, 389 U.S. 347 (1967).

¹¹ 18 U.S.C. § 2518.

¹² *United States v. New York Tel. Co.*, 434 U.S. 159, 167 (1977).

pen register did not implicate privacy interests protected under the Fourth Amendment. The Supreme Court began its analysis in *Smith* by noting that “a pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the contents of communications.”¹³ Further emphasizing the minimal nature of the information collected by a pen register, the Supreme Court went on:

Indeed, a law enforcement official could not even determine from the use of a pen register whether a communication existed. These devices do not hear sound. They disclose only the telephone numbers that have been dialed -- a means of establishing communication. Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers.¹⁴

The Supreme Court concluded that “telephone users, in sum, typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes.”¹⁵ Therefore, given the “limited capabilities” of a pen register, an individual has no “‘legitimate expectation of privacy’ regarding the numbers he dialed on his phone.”¹⁶ Accordingly, the Supreme Court in *Smith* hinged its view of pen register interceptions on the distinction between the content of communications and the “numbers dialed.”¹⁷

¹³ *Smith*, 442 U.S. at 741.

¹⁴ *Id.* (quoting *New York Tel. Co.*, 434 U.S. at 167). The Supreme Court in *New York Tel. Co.* had also explained:

[P]en registers do not accomplish the ‘aural acquisition’ of anything. They decode outgoing telephone numbers by responding to changes in electrical voltage caused by the turning of the telephone dial (or the pressing of buttons on pushbutton telephones) and present the information in a form to be interpreted by sight rather than by hearing. *New York Tel. Co.*, 434 U.S. at 167.

¹⁵ *Smith*, 442 U.S. at 743.

¹⁶ *Id.* at 742.

¹⁷ Other commentators have similarly described the narrow nature of pen registers:

While the *Smith* decision made clear that the Fourth Amendment did not cover pen registers, the Supreme Court left open the question of what authority, short of a probable cause order, was required to compel a telephone company to install a pen register or trap and trace device. In 1986, as part of ECPA, Congress answered this question by adopting standards for the authorization of pen registers and trap and trace devices. The Senate Judiciary Committee took the same narrow view of pen registers and trap and trace devices that had influenced the Supreme Court:

Briefly, a pen register is a device which can be attached to a telephone line for the purpose of decoding and recording the numbers dialed from that line. A trap and trace device is used to identify the originating number of an incoming wire or electronic communication. These devices do not identify or record the contents of the communication.¹⁸

Consequently, the statutory definitions of pen register and trap and trace device in ECPA are narrowly drawn:

the term 'pen register' means a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached . . . ;

the term 'trap and trace device' means a device which captures the incoming electronic or other impulses which identify the originating number of an

A pen register is a mechanical device, usually installed in a central telephone company facility, that records on paper the numbers dialed from a particular telephone. It reveals only the numbers that have been dialed; it does not enable anyone to hear anything that is being said. It does not reveal who placed the call, nor who received the call, nor even whether the call was completed; all it reveals is that someone used the monitored phone to attempt to reach someone at the number dialed. Clifford S. Fishman, Professor of Law at the Catholic University of America Law School, testimony before the Subcomm. on Courts, Civil Liberties and the Administration of Justice, House Judiciary Committee, March 5, 1986, p. 259-60.

See also *Electronic Surveillance Report*, National Wiretap Commission, 1976 at 120 ("The pen register is a device which can be attached to a telephone line to record dialing impulses and thus the telephone number dialed by an outgoing call. It does not indicate whether the call was completed The pen register merely produces a paper tape which is perforated as the numbers are dialed, and from which the number called can be determined.")

¹⁸ S. Rep. No. 99-541, at 46 (1986)("Senate Report").

instrument or device from which a wire or electronic communication was transmitted.¹⁹

And since these definitions are so narrow in scope, Congress ultimately adopted in ECPA a standard for pen registers that is essentially a rubber stamp. The standard requires a judge to approve any application for a pen register that is signed by any federal prosecutor, or any state or local police officer, attesting that the “information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.”²⁰ The Committee Reports of both the House and Senate Judiciary Committees specifically noted that “[t]his provision does not envision an independent judicial review of whether the application meets the relevance standard, rather the court needs only to review the completeness of the certification submitted.”²¹

None of the special protections that Congress imposed on wiretapping in Title III apply to pen registers. For example, pen register orders are not limited to investigations of serious offenses, high level Justice Department review of the application is not required, and prior exhaustion of other investigative techniques (pen registers and trap and trace devices are often used at the starting point of an investigation) is not mandated. Furthermore, while Title III orders are issued for 30 days, and must be terminated as soon as the investigative objective is accomplished, pen register orders run for 60 days. And, once the order is approved, there is no ongoing judicial supervision and no return of service to the court.

¹⁹ 18 U.S.C. § 3127(3) and (4).

²⁰ 18 U.S.C. § 3123(a).

²¹ Senate Report at 47.

B. The Government's Approach to CALEA Would Impermissibly Expand Information Available Under a Pen Register Authorization

CDT is not asking the Commission to question the very low standard and lack of judicial supervision for pen registers and trap and trace devices. That is obviously a matter for Congress. However, the minimal privacy protections for pen registers are based on the assumption that they record dialed numbers only. Yet the government's approach to CALEA, unless rejected by this Commission, would impermissibly expand the amount of information that law enforcement would receive under mere pen register and trap and trace authority.

Essentially, the government is attempting to use CALEA to include more data in the category of "call-identifying information," which will ensure that such data can be available under the lower pen register standard. While this is clearly an issue with respect to the punch list items, it raises particularly grave concerns in the context of the industry standard's treatment of electronic surveillance in packet environments. The interim industry standard allows law enforcement agencies, possessing only the rubber-stamp authority of a pen register order, to receive all of the content of a person's communications without any effort by carriers to separate the "dialed numbers" from the content. Accordingly, the treatment of packet transmission in the industry standard threatens to obliterate entirely the distinction between content and "dialed numbers" or similar signaling information.

The FBI and DOJ argue that Title III's "minimization" requirement is adequate to protect the acquisition of the content of packet communications under a pen register order. However, this assertion is simply wrong because there is no "minimization" requirement under the pen register standard, nor are there many of the other privacy protections contained in Title III. Title III requires that "[e]very order . . . shall contain a provision that the authorization to intercept . . .

shall be conducted in such a way as to *minimize* the interception of communications not otherwise subject to interception”²² In addition, Title III provides that the authorizing judge may require periodic reports showing what progress has been made toward the authorized objective and whether it is necessary to continue the interception.²³ Finally, Title III requires in all cases that there be a return to the authorizing judge of all interception tapes.²⁴ ECPA contains none of these protections for pen register orders.

Perhaps the clearest indication that Congress did not consider Title III and ECPA’s privacy protections sufficient to deal with current technologies and the new obligations imposed by CALEA is found in the fact that CALEA included a specific privacy protection requirement of its own, Section 103(a)(4). Section 103(a)(4) requires carriers to protect the privacy and security of communications not authorized to be intercepted. This protection was not added to Title III or ECPA. Rather, it is a requirement intended to limit what carriers must do to accommodate the government’s interest in a sustained wiretap capability. This requirement, unlike the other design requirements in CALEA, is intended as a counterbalance to the pro law enforcement requirements of Section 103(a)(1) - (3). This entirely new requirement on telecommunications carriers directs them to design their systems in such a way as to withhold from law enforcement the content of communications that law enforcement has no authority to intercept. The interim standard’s application to packet networks is therefore deficient because it fails to require network design that would separate content from addressing or signaling information.

²² 18 U.S.C. § 2518(5)(emphasis added).

²³ 18 U.S.C. § 2518(6).

²⁴ 18 U.S.C. § 2518(8)(a).

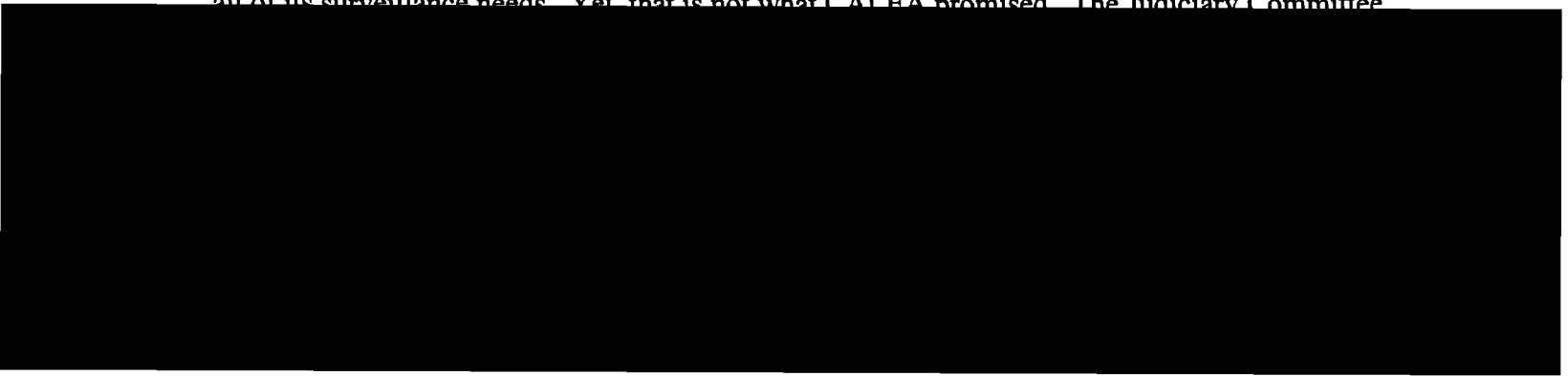
Whether or not it is appropriate to make some provision for packet networks in the CALEA standard, there is no question that the interim standard's treatment of packet networks is deficient as a matter of law. To the extent the Commission concludes that packet networks may have a place in the CALEA standard, far more study is needed, including the participation of expert standard-setting bodies such as the Internet Engineering Task Force, in order to properly address this critical issue of privacy on data networks.

II. THE GOVERNMENT FAILS TO RECOGNIZE CALEA'S BUILT-IN LIMITATIONS

CALEA was intended to ensure that law enforcement was not precluded from acquiring call content and call-identifying information on a suspect. It was not intended to make this information available in the most convenient way from a single carrier or under a single order.

Congress wrote this principle directly into the language of the statute. Section 108(a)(1) provides that a court may not issue a compliance order against a carrier if "the facilities of another carrier are . . . reasonably available to law enforcement for implementing the interception of communications or access to call-identifying information."²⁵ Thus, if the requested capability is otherwise reasonably available to law enforcement from another carrier, the requirements of CALEA are satisfied.

The FBI, however, wants one-stop shopping. In a way, the government wants to turn back the clock not on technology, but on the divestiture of AT&T, providing a single source for all of its surveillance needs. Yet, that is not what CALEA promised. The Judiciary Committee



explicitly stated that “[t]he bill is not intended to guarantee ‘one-stop shopping’ for law enforcement.”²⁶

Similarly, Congress did not intend to extend CALEA’s capability assistance requirements as broadly as the reach of the wiretap laws. For example, Congress omitted in CALEA whole categories of service providers that are covered by Title III and ECPA. In addition, the term “telecommunications carrier” in CALEA is far narrower than “provider of wire or electronic communication service” in Title III. Furthermore, CALEA excludes entire categories of service providers, including Internet service providers and operators of switch boards. CALEA also does not include all of the types of services covered by Title III and ECPA, notably information services. And, finally, CALEA does not encompass all signaling and dialing information, but only signaling and dialing information “that identifies the origin, direction, destination or termination of a communication.” The government is simply wrong that CALEA requires that telecommunication networks be capable of readily providing access to all information that can be legally intercepted under Title III.

The principle that CALEA does not require one carrier to make modifications in its system to provide what is already available from another carrier is relevant to two of the more hotly-contested punch list items: conference calling and post cut-through digits. These punch list capabilities find no support in the language of the Act. At the same time, the failure to provide for these capabilities in a CALEA standard in no way prevents law enforcement access to the type of information that government seeks to capture. Rather, law enforcement is merely required to pursue alternative, but nonetheless available, sources for such information.

²⁶ H.R. Rep. No. 103-827, at 22 (1994)(“House Report”).

For example, if a target of electronic surveillance calls A and B, conferences them together, and then drops off, and law enforcement believes that A and B discuss criminal conduct, then law enforcement can obtain a Title III intercept order against the facilities of A or B, assuming it can show probable cause to believe they are engaged in criminal conduct using their telephones.²⁷ Law enforcement does not lose the evidence to which it is entitled, if it goes through the procedure of obtaining the necessary order.²⁸ The requirements of CALEA are met without requiring any carrier to redesign its system to capture all of the conversations under one order.

Likewise, the same principle also shows why the government is wrong in its approach to post cut-through dialed digits. Contrary to the government's assertion, CDT's position would not "effectively foreclose carriers from providing dialing information used to complete calls."²⁹ The FBI wants the local carrier to provide, under a pen register, the information dialed after call cut-through to a long distance carrier. There is no doubt that if the FBI went to the second, long distance carrier, it could get the post cut-through dialed digits, under the pen register standard.³⁰ If the information in question is reasonably available from an identified service provider, which is all that CALEA requires, law enforcement should go there. The government may argue there

²⁷ If law enforcement cannot establish probable cause of criminal conduct as to either A or B over the facilities of either, then it should not be intercepting their communications in the first place.

²⁸ Indeed, it would seem that law enforcement would be well advised to obtain an order for the facilities of either A or B or both, since if it has probable cause to believe that they are engaged in criminal conduct, then it would want to intercept their communications not only with each other, but with C and D and so on, to determine the full scope of the criminal enterprise.

²⁹ FBI/DOJ Comments at 11-12, n. 2.

³⁰ Again, it would seem to be to law enforcement's advantage to go to the long distance carrier with a pen register order, for then the government could obtain all of the "post cut-through dialed digits," regardless of where the subject was when he accessed the long distance service.

could be inconvenience in such circumstances, but this is an argument that must be made to Congress, not the carriers or this Commission.

III. CALEA MUST BE NARROWLY INTERPRETED IN ACCORDANCE WITH ITS PLAIN MEANING

The Commission has a responsibility to preserve the balance between privacy and law enforcement interests that has always governed Congress' approach to the sensitive issue of wiretapping. To preserve the balance when implementing CALEA, a careful adherence to the words of the statute, interpreted in context, is required. A surveillance capability not clearly mandated by the words of the statute has no place in an industry or Commission safe harbor standard. To allow any such capability to be implemented would upset the delicate balance Congress historically sought in the wiretap statutes and, once again, achieved in CALEA.

Given the serious privacy interests at stake, it is especially important that the Commission adhere closely to the words of the statute. Moreover, Congress has indicated its expectation that the Commission will narrowly interpret the Act's requirements.³¹ Anything else will involve the Commission in endless judgment calls as to what is "essential" to law enforcement.

The government, however, does not stick closely to the words of the statute. Instead, it attempts to include words that are not present in the Act. In addition, the government gives a word in a given phrase multiple meanings to suit its objectives. Sometimes, the government even ignores the words of the Act altogether, arguing that the Commission should do what is best to serve the needs or even the conveniences of law enforcement.

³¹ "The Committee expects industry, law enforcement and the FCC to narrowly interpret the [capability assistance] requirements." House Report at 23.

A. Words Cannot be Added to the Act

In several cases, the government can only justify its arguments for enhanced capabilities by adding extraneous words to the statute. For example, to support its demand for conference calling capabilities, the government reads into the statute the words “supported by the subscriber’s service or facility.”³² The statute, however, does not cover communications “supported by” the subscriber’s service or facility. The statute only covers communications “to or from” the subscriber’s equipment, facility, or service.

Similarly, to justify its claims that party join, party hold and party drop messages are mandated by CALEA, the government reads the Act as requiring call-identifying information on each “leg of a call.” The statute, however, does not require carriers to break down calls into “legs.” CALEA only requires carriers to provide “dialing or signaling information that identifies the origin, direction, destination, or termination *of each communication . . .*”

To further justify its claim regarding subject-initiated dialing and signaling activity (*e.g.*, flash hooks), the government adds to the statute a requirement to identify the parties to a communication. But, once again, the Act does not require carriers to identify “parties,” it requires carriers to provide dialing or signaling information that identifies the “origin, direction, destination, or termination of each communication.”³³

B. A Particular Word in a Particular Clause Cannot have Multiple Meanings

A word can be used differently in different parts of a statute. However, a single use of a word cannot have multiple meanings. Yet, this is precisely what the government must argue to support its demand for location information. The government recognizes that location

³² FBI/DOJ Petition at ¶¶ 46, 55.

information is required only if it can be found within the meaning of call-identifying information. And Congress defined call-identifying information as information “that identifies the origin, direction, destination, or termination of each communication.”³⁴ To properly interpret the statutory language, each of these words must be given a single, distinct meaning. Clearly, origin refers to the number of the calling party, and destination refers to the number of the called party. But in the case of wireless calls, the government would have “destination” mean not only the number of the called party, but *also* the cell site of the called party as well. In addition, the government would have “origin” mean not only the number of the calling party, but *also* the cell site of the calling party.

Indeed, the confusion that would be caused by giving these words the multiple meanings attributed to them by the government is even more complicated than that described above. Under the government’s reading, “destination” would mean the cell site of the called party when the called party is the subject of the surveillance (the government does not need a trap and trace device to tell it the number of the called party when the called party’s line is being monitored). But “destination” would mean the number of the called party when the subject of the surveillance is the calling party (the calling party’s switch where the intercept is effected has no information indicating where the called party is physically located).

IV. THE GOVERNMENT’S APPROACH TO CONFERENCE CALLS VIOLATES FUNDAMENTAL TITLE III PRINCIPLES

The government wants phone companies to design their systems so the government can continue monitoring parties to a multi-party call even after the subject named in the intercept

³³ 47 U.S.C. § 1001(2)(emphasis added).

order is no longer participating in the call, but has dropped off to make another call that is being intercepted.

Title III, incorporating the Fourth Amendment's requirement of particularity, does not allow this type of general search and seizure of the communications of parties based on their having had a conversation with a target of criminal investigation. If the government wants to monitor the communications of persons (or phone lines) that used to be, but no longer are in communication with the person (or phone line) that is the subject of a Title III order, it must show probable cause to believe that those other persons (or those other phone lines) are engaged in the commission of a crime and a new Title III order must be obtained.

Consider one scenario that the government wants to cover: A is the focus of criminal investigation. The government has established probable cause to believe that A is involved in a particular criminal offense and that A's phone line is being used in the commission of that offense and has obtained a Title III order on A's phone line. A sets up a conference call with B and C using the conference call capability provided by A's service provider. Then A puts B and C on hold (or hangs up entirely) and calls D. The government clearly would want to listen to A's new conversation with D, since A is the subject of investigative interest, and thus J-STD requires carriers to intercept A's conversation with D. But the government also claims that CALEA mandates the ability to simultaneously intercept the continuing conversation between B and C.

This is where government stretches the constitutional principle of particularity beyond its breaking point.

³⁴ *Id.*

It is important to note that the government is not arguing here that the intercepted facility is the conference calling facility, for the government does not want the interception merely to follow the conference call. Rather, the government maintains that A's phone line remains the targeted facility, for they want, with a single Title III order, to be able to monitor simultaneously both the conference calling facility and the original phone line. This is what the Fourth Amendment and Title III do not allow.

The Fourth Amendment requires that any warrant "particularly describ[e] the place to be searched, and the person or things to be seized." This "particularity" requirement is embodied in Title III.³⁵ It requires either the specification of a named person to be searched or of a named facility. The Supreme Court has held that conversations of unnamed parties speaking with the party named in an order can be constitutionally intercepted. And the Court has held that the conversations of unnamed parties using the phone line specified in the order can be constitutionally intercepted. For example, the gambler's spouse who uses the phone named in the order can be intercepted.³⁶ Finally, the courts have allowed the government to tap an unspecified facility under the so-called "roving tap" authority so long as it is limited to the interception of conversations of the named subject. But the courts have never approved what the government seeks here: the interception of unnamed persons using unspecified facilities, while the named person is being intercepted on the specified facility, just because the unnamed persons previous had been using that facility as well.

³⁵ 18 U.S.C. § 2518(1)(b) and (3).

³⁶ See *United States v. Kahn*, 415 U.S. 143 (1974).

For Fourth Amendment purposes, it is irrelevant who pays for the conference calling capability. “We are not inclined to make a crazy quilt of the Fourth Amendment, especially in circumstances where (as here) the pattern of protection would be dictated by billing practices of a private corporation.”³⁷

The government has a clear option: once they find that A is making conference calls to B and C, which are believed to involve criminal conduct, the government can seek an order against the phone line of either B or C. If probable cause can be shown to believe that the phone line of B or C is being used for criminal purposes, an order will issue. (That order, by the way, will authorize the interception of all conversations over the newly target facility, not merely those that began as conference calls set up by A.)

This is another case in which the government is trying to mandate one-stop shopping. Not only is it one-stop shopping that CALEA does not require, but it is one-stop shopping that the Constitution does not permit.

One final point. The government cites in its May 20 comments a portion of the following passage from CALEA’s legislative history:

The purpose of H.R. 4922 [the bill that became CALEA] is to preserve the government’s ability, pursuant to court order or other lawful authorization, to intercept communications involving advanced technologies such as digital or wireless transmission modes, or features and services such as call forwarding, speed dialing and conference calling, while protecting the privacy of communications and without impeding the introduction of new technologies, features, and services.³⁸

³⁷ *Smith*, 442 U.S. at 745.

³⁸ FBI/DOJ Comments at ¶ 12.